<u>IN THE CLAIMS</u>:

A status of all the claims of the present Application is presented below:

1. **(Currently Amended)**   A method for secure data transmission, comprising:

generating a character string at a sender <u>for each data packet associated with the</u> <u>secure data transmission</u>;

generating a hash key using the character string and a private key<u>, wherein the hash</u> <u>key is different for each data packet associated with the secure data transmission</u>;

encrypting [[the]] <u>a</u> data <u>packet associated with the secure data transmission</u> using the hash key; and

transmitting an identification key associated with the sender, the character string, and the encrypted data <u>packet</u> from the sender to a recipient.

2. **(Original)** The method of Claim 1, wherein generating the hash key comprises hashing the character string with the private key.

3. **(Original)** The method of Claim 1, further comprising:

generating a signature using the hash key and the data; and

transmitting the signature from the sender to the recipient.

4. **(Original)** The method of Claim 1, wherein generating a character string comprises randomly generating the character string.

5. **(Original)** The method of Claim 1, further comprising:

determining the private key at the recipient using the identification key; and

decrypting the encrypted data at the recipient using the private key and the character string.

6. **(Original)** The method of Claim 5, wherein determining the private key comprises accessing a relational database associating the identification key to the private key.

7. **(Original)** The method of Claim 1, further comprising:

determining the private key at the recipient using the identification key;

determining the hash key at the recipient using the private key and the character string; and

decrypting the encrypted data using the hash key.

8. **(Original)** The method of Claim 7, wherein determining the hash key comprises hashing the private key with the character string.

9. **(Original)** The method of Claim 1, further comprising:

generating a first signature by the sender using the hash key and the data; and

transmitting the first signature to the recipient, the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data.

10. **(Original)** The method of Claim 1, further comprising:

generating a signature using the hash key and the data;

transmitting the signature to the recipient;

determining the private key at the recipient using the identification key;

determining the hash key at the recipient using the private key and the character string;

decrypting the encrypted data at the recipient using the hash key; and

verifying the signature at the recipient using the hash key and the decrypted data.

11. **(Currently Amended)** A method for secure data transmission, comprising:

receiving a <u>plurality of</u> character ~~string~~ <u>strings</u> from a sender;

receiving an identification key from the sender;

receiving <u>a plurality of</u> encrypted data <u>packets</u> from the sender<u>, each of the plurality of character strings correspond to one of the plurality of encrypted data packets</u>;

determining a private key associated with the sender using the identification key; and

decrypting the <u>plurality of</u> encrypted data <u>packets</u> using the private key and the <u>respective</u> character ~~string~~ <u>strings</u>.

12. **(Original)** The method of Claim 11, further comprising determining a hash key using the character string and the private key, and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key.

13. **(Original)** The method of Claim 11, wherein determining the private key comprises accessing a relational database associating the identification key to the private key.

14. **(Original)** The method of Claim 11, wherein receiving the character string comprises receiving a randomly generated character string.

15. **(Original)** The method of Claim 11, further comprising hashing the character string with the private key to generate a hash key, and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key.

16. **(Original)** The method of Claim 11, further comprising:

receiving a signature from the sender; and

verifying the signature using the decrypted data, the private key, and the character string.

17. **(Original)** The method of Claim 11, further comprising:

receiving a signature from the sender;

determining a hash key using the private key and the character string; and

verifying the signature using the decrypted data and the hash key.

18. **(Original)** The method of Claim 11, further comprising:

receiving a first signature from the sender;

determining a hash key using the private key and the character string;

generating a second signature using the hash key and the decrypted data; and

comparing the first signature to the second signature.

19. **(Currently Amended)**   A system for secure data transmission, comprising:

a processor;

a memory coupled to the processor;

a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string;

a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the character string and a private key, wherein the hash key is different for each data packet associated with the secure data transmission; and

an encryption engine stored in the memory and executable by the processor, the encryption engine adapted to encrypt the data using the hash key; and

wherein the processor is adapted to transmit the encrypted data, an identification key related to the private key, and the character string to a recipient.

20. **(Original)** The system of Claim 19, further comprising a signature engine stored in the memory and executable by the processor, the signature engine adapted to generate a signature using the hash key and the data, the processor further adapted to transmit the signature to the recipient

21. **(Original)** The system of Claim 20, wherein the recipient is adapted to decrypt the encrypted data and verify the signature using the decrypted data.

22. **(Original)** The system of Claim 19, wherein the hashing engine is adapted to hash the character string with the private key to generate the hash key.

23. **(Original)** The system of Claim 19, wherein the string generator is adapted to randomly generate the character string.

24. **(Original)** The system of Claim 19, wherein the recipient is adapted to decrypt the encrypted data using the identification key and the character string.

25. **(Original)** The system of Claim 19, wherein the recipient is adapted to determine the hash key using the identification key and the character string and decrypt the encrypted data using the hash key.

26. **(Original)** The system of Claim 19, wherein the recipient is adapted to access a relational database associating the identification key with the private key and decrypt the encrypted data using the private key and the character string.

27. **(Currently Amended)**   A system for secure data transmission, comprising:

a processor adapted to receive a plurality of encrypted data packets, an identification key, and a plurality of character string strings from a sender, each of the plurality of character strings correspond to one of the plurality of encrypted data packets;

a memory coupled to the processor;

a relational database stored in the memory and accessible by the processor, the relational database relating the identification key to a private key; and

a decryption engine stored in the memory and executable by the processor, the decryption engine adapted to decrypt the encrypted data <u>packets</u> using the <u>respective</u> character ~~string~~ <u>strings</u> and the private key.

28. **(Original)** The system of Claim 27, further comprising a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key and the character string, the decryption engine adapted to decrypt the encrypted data using the hash key.

29. **(Original)** The system of Claim 27, further comprising a signature engine stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the private key and the character string.

30. **(Original)** The system of Claim 27, further comprising:
a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key and the character string; and
a signature engine stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the hash key and the decrypted data.

31. **(Original)** The system of Claim 27, further comprising a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string with the private key to generate a hash key, the decryption engine adapted to decrypt the encrypted data using the hash key.

32. **(Original)** The system of Claim 27, further comprising a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string, and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the character string and the private key.

33. **(Previously presented)** The system of Claim 32, further comprising:
a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string; and
a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string with the private key to generate a hash key, and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the hash key.

34. **(Original)** The system of Claim 32, further comprising a signature engine stored in the memory and executable by the processor, the signature engine adapted to generate a first signature using the decrypted data and compare the first signature to a second signature received from the sender.